Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 26 juillet 2001
N° CERTA-2001-AVI-082

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le serveur Terminal sous Windows NT et 2000

Gestion du document

Référence	CERTA-2001-AVI-082
Titre	Vulnérabilité dans le serveur Terminal sous Windows NT et 2000
Date de la première version	26 juillet 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-040
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Déni de Service

2 Systèmes affectés

- Microsoft Windows NT 4.0 Terminal Server Edition ;
- Microsoft Windows 2000 Server ;
- Microsoft Windows 2000 Advanced Server ;
- Microsoft Windows 2000 Datacenter Server.

3 Résumé

Une vulnérabilité présente dans le serveur Terminal permet à un utilisateur distant mal intentionné d'épuiser les ressources de la machine cible.

4 Description

Le serveur de terminal permet de déporter un environnement sur une machine distante. Ce service utilise le port 3389/TCP.

Un utilisateur distant mal intentionné peut, par le biais de requêtes RDP (Remote Data Protocol) astucieusement composées, provoquer une fuite de mémoire sur la machine offrant ce service. Un nombre important de ces requêtes peut obliger un redémarrage du serveur.

5 Contournement provisoire

Bloquer le port 3389/TCP au niveau du garde barrière afin d'empêcher l'exécution de cette vulnérabilité depuis l'Internet.

6 Solution

Télécharger le correctif disponible sur le site Microsoft :

- Microsoft Windows NT 4.0 Terminal Server Edition :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31615
- Microsoft Windows 2000 :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30195
- Microsoft Windows 2000 Datacenter Server :
  Concernant Microsoft Windows 2000 Datacenter Server, Microsoft préconise de prendre contact avec le fournisseur du serveur afin de connaître les solutions à apporter.

7 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-040.asp

Gestion détaillée du document

26 juillet 2001 version initiale.